IN THE CLAIMS

Complete listing of the claims:

1. (Previously presented) A method for securely communicating information, comprising:

optically encrypting said information and storing the resulting encrypted data;

reading out the encrypted data in the spatial domain and converting said encrypted data to the temporal domain;

transmitting the converted encrypted data;

receiving the transmitted encrypted data and converting the received encrypted data to the spatial domain using threshold sampling to avoid overlap between adjacent data in the transmitted encrypted data; and

decrypting the converted received encrypted data to recover said information

2. (Previously presented) The method as defined by claim 1, wherein said reading out the encrypted data in the spatial domain and converting the encrypted data to the temporal domain is implemented using ultrafast laser pulses.

3. (Previously presented) The method as defined by claim 1, wherein said reading out the encrypted data in the spatial domain and converting the encrypted data to the temporal domain is implemented using ultrafast laser pulses spread in the spatial domain according to their spectral components.

4. (Original) The method as defined by claim 3, wherein said ultrafast pulses are spread in the spatial domain by diffraction.

5. (Previously presented) The method as defined by claim 2, wherein said transmitting the converted data comprises transmitting said converted data over an optical network.

6. (Previously presented) The method as defined by claim 2, wherein said converting received encrypted data to the spatial domain is implemented using ultrafast laser pulses.

7. (Original) The method as defined by claim 2, wherein said optical encryption includes random phase encryption.

8. (Original) The method as defined by claim 2, wherein said optical encryption includes double random phase encryption.

9. (Original) The method as defined by claim 8, wherein said double random phase encryption includes phase encryption in the spatial domain and phase encryption in the frequency domain.

10. (Original) The method as defined by claim 2, wherein said storing of encrypted data comprises holographically storing said encrypted data.

11. (Previously presented) The method as defined by claim 2, wherein said reading out and converting said encrypted data comprises:

forming a real-time hologram using read-out encrypted data and a reference beam;

reading out the real-time hologram; and

converting the read-out hologram from the spatial domain to the temporal domain.

12. (Previously presented) The method as defined by claim 11, wherein said reading out the real-time hologram comprises directing a diffracted ultrafast laser pulse at said real time hologram.

13. (Previously presented) The method as defined by claim 5, wherein said reading out and converting said encrypted data comprises:

forming a real-time hologram using read-out encrypted data and a reference beam;

reading out the real-time hologram; and

converting the read-out hologram from the spatial domain to the temporal domain.

14. (Previously presented) The method as defined by claim 13, wherein said reading out the real-time hologram comprises directing a diffracted ultrafast laser pulse at said real time hologram.

15. (Previously presented) The method as defined by claim 6, wherein said decrypting the converted received encrypted data includes phase decoding of said converted received encrypted data.

16. (Previously presented) The method as defined by claim 6, wherein said decrypting the converted received encrypted data includes phase decoding of said converted received encrypted data in the spatial domain and in the frequency domain.

17. (Previously presented) A method for securely transmitting information, comprising:

optically encrypting said information and storing the resulting encrypted data;
reading out the encrypted data in the spatial domain, and converting said encrypted data to the temporal domain using threshold sampling to avoid overlap between adjacent data in the encrypted data; and
transmitting the converted encrypted data.

18. (Previously presented) The method as defined by claim 17, wherein said reading out the encrypted data in the spatial domain and converting the encrypted data to the temporal domain is implemented using ultrafast laser pulses.

19. (Previously presented) The method as defined by claim 17, wherein said reading out the encrypted data in the spatial domain and converting the encrypted data to the temporal domain is implemented using ultrafast laser pulses spread in the spatial domain according to their spectral components.

20. (Original) The method as defined by claim 18, wherein said optical encryption includes random phase encryption.

21. (Original) The method as defined by claim 18, wherein said optical encryption includes double random phase encryption.

22. (Original) The method as defined by claim 18, wherein said double random phase encryption includes phase encryption in the spatial domain and phase encryption in the frequency domain.

23. (Original) The method as defined by claim 18, wherein said storing of encrypted data comprises holographically storing said encrypted data.

24. (Previously presented) The method as defined by claim 17, wherein said reading out and converting said encrypted data comprises:

forming a real-time hologram using read-out encrypted data and a reference beam;

reading out the real-time hologram; and

converting the read-out hologram from the spatial domain to the temporal domain.

25. (Previously presented) The method as defined by claim 24, wherein said reading out the real-time hologram comprises directing a diffracted ultrafast laser pulse at said real time hologram.

26. (Previously presented) Apparatus for securely communicating information, comprising:

means for optically encrypting said information and storing the resulting encrypted data;

means for reading out the encrypted data in the spatial domain, and converting said encrypted data to the temporal domain;

means for transmitting the converted encrypted data;

means for receiving the transmitted encrypted data and converting the received encrypted data to the spatial domain; and

means for decrypting the converted received encrypted data to recover said information using threshold sampling to avoid overlap between adjacent data in the converted encrypted data.

27. (Original) Apparatus as defined by claim 26, wherein said means for receiving the transmitted encrypted data and converting the received encrypted data to the spatial domain includes diffracted ultrafast laser pulses.

28. (Original) Apparatus as defined by claim 27, wherein said means for optically encrypting includes means for implementing double random phase encryption.

29. (Previously presented) For use in conjunction with a method for securely communicating information that includes the steps of: optically encrypting said information and storing the resulting encrypted data; reading out the encrypted data in the spatial domain, and converting said encrypted data to the temporal domain; and transmitting the converted encrypted data; a receiver subsystem, comprising:

means for receiving the transmitted encrypted data and converting the received encrypted data to the spatial domain; and

means for decrypting the converted received encrypted data to recover said information using threshold sampling to avoid overlap between adjacent data in the converted received encrypted data.

30. (Original) The receiver subsystem as defined by claim 29, wherein said means for receiving the transmitted encrypted data and converting the received encrypted data to the spatial domain includes diffracted ultrafast laser pulses.

31. (Currently amended) For use in a method for securely communicating information, wherein said information has been optically encrypted and the resultant encrypted data has been stored, the method comprising:

reading out the encrypted data in the spatial domain, and converting said encrypted data to the temporal domain;

transmitting the converted encrypted data;

receiving the transmitted encrypted data and converting the received encrypted data to the spatial domain; and

decrypting the converted received encrypted data to recover said information using threshold sampling to avoid overlap between adjacent data in the converted encrypted data.

32. (Original) The method as defined by claim 31, wherein said step of reading out the encrypted data in the spatial domain and converting the encrypted data to the temporal domain is implemented using ultrafast laser pulses.

33. (Original) The method as defined by claim 31, wherein said step of reading out the encrypted data in the spatial domain and converting the encrypted data to the temporal domain is implemented using ultrafast laser pulses spread in the spatial domain according to its spectral components.

34. (Original) The method as defined by claim 31, wherein said stored encrypted data comprises holographically stored encrypted data, and wherein said step of reading out and converting said encrypted data includes:

forming a real-time hologram using read-out encrypted data and a reference beam;

reading out the real-time hologram; and

converting the read-out hologram from the spatial domain to the temporal domain.

35. (Original) The method as defined by claim 34, wherein said step of reading out the real-time hologram comprises directing a diffracted ultrafast laser pulse at said real time hologram.